

# PATENT COOPERATION TREATY

From the:  
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

**RECEIVED**  
**MATHYS & SQUIRE**

- 9 JUL 1999

REPLY DATE 7/10/99

Reply Written Opin  
DIARY ENTERED

**PCT**

WRITTEN OPINION

(PCT Rule 66)

To:  
COZENS, P.  
MATHYS & SQUIRE  
100 Gray's Inn Road  
London WC1X 8AL  
GRANDE BRETAGNE

Date of mailing  
(day/month/year)

07.07.99

Applicant's or agent's file reference  
PDC/AB/20099

**REPLY DUE**

**within 3 month(s)**  
from the above date of mailing

International application No.  
PCT/IB98/01610

International filing date (day/month/year)  
02/10/1998

Priority date (day/month/year)  
02/10/1997

International Patent Classification (IPC) or both national classification and IPC  
H04N7/16

Applicant  
CANAL+ SOCIETE ANONYME et al.

1. This written opinion is the **first** drawn up by this International Preliminary Examining Authority.

2. This opinion contains indications relating to the following items:

- I ☒ Basis of the opinion
- II ☐ Priority
- III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain document cited.
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

3. The applicant is hereby **invited to reply** to this opinion.

**When?** See the time limit indicated above. The applicant may, before the expiration of that time limit, request this Authority to grant an extension, see Rule 66.2(d).

**How?** By submitting a written reply, accompanied, where appropriate, by amendments, according to Rule 66.3. For the form and the language of the amendments, see Rules 66.8 and 66.9.

**Also:** For an additional opportunity to submit amendments, see Rule 66.4.  
For the examiner's obligation to consider amendments and/or arguments, see Rule 66.4 bis.  
For an informal communication with the examiner, see Rule 66.6.

**If no reply is filed,** the international preliminary examination report will be established on the basis of this opinion.

4. The final date by which the international preliminary examination report must be established according to Rule 69.2 is: **02/02/2000.**

Name and mailing address of the international preliminary examining authority:



European Patent Office  
D-80298 Munich  
Tel. (+49-89) 2399-0 Tx: 523656 epmu d  
Fax: (+49-89) 2399-4465

Authorized officer / Examiner

Schoeyer, M

Formalities officer (incl. extension of time limits)  
Schmethusen, S  
Telephone No. (+49-89) 2399 2667 2432



**I. Basis of the opinion**

1. This opinion has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this opinion as "originally filed".*):
  
2. The amendments have resulted in the cancellation of:
  - ☐ the description,      pages:
  - ☐ the claims,          Nos.:
  - ☐ the drawings,        sheets:
  
3. This opinion has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):
  
4. Additional observations, if necessary:

**III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability**

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been and will not be examined in respect of:

- ☐ the entire international application,
- ☒ claims Nos. 22,23;

because:

- ☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (*specify*):
  
- ☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. are so unclear that no meaningful opinion could be formed (*specify*):  
  
**see separate sheet**
  
- ☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.
  
- ☐ no international search report has been established for the said claims Nos. .

**V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement****1. Statement**

Novelty (N)	Claims	NO: 1, 14,15,17,19,20,21
Inventive step (IS)	Claims	No: 2-13,16,18
Industrial applicability (IA)	Claims	YES: 1-21

**2. Citations and explanations****see separate sheet****VII. Certain defects in the international application**

The following defects in the form or contents of the international application have been noted:

**see separate sheet****VIII. Certain observations on the international application**

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

**see separate sheet**

**III. Non Establishment of Opinion**

The subject-matter of claims 22 and 23 is not defined in a proper way. None of the features of these claims actually define any subject-matter.

In the case of claim 22 it has not been claimed in what way the decoder and portable security module are adapted, while in claim 23 reference is made to application as a whole without defining any subject-matter to be protected.

**V. Statement under Rule 66.2(a)(ii)**

Reference is made to the following documents:

D1: WO 96 06504 A (THOMSON CONSUMER ELECTRONICS ;CHANNEY JOHN WILLIAM (US)) 29 February 1996;

**Article 33(2) PCT**

As far as the subject-matter of the claims can be understood (see under VIII), independent claim 1 does not fulfil the requirements of Article 33(2) PCT because the subject-matter of independent claim 1 is not novel.

Document D1 (see abstract) is concerned with a method of transmission and reception of a scrambled data streams and discloses:

- transmission of the scrambled data stream to a decoder and passing it on to and descrambling by a portable security module inserted in the decoder;
- passing of data stream from the security module to the decoder in an encrypted for, to be decrypted and subsequently used by the decoder.

Since these are the features of claim 1, the subject-matter of claim 1 lacks novelty.

Dependent claims:

The subject-matter of some of the dependent claims also lacks novelty as will be set out below:

Claim 14:

Document D1 discloses (see page 22), that the signal is encrypted with a key at transmission and decrypted in the receiver with the equivalent decryption key;

- encryption based on variable known to both the transmitter and the decoder (as in claim 15), -see D1 (page 2, line 22 ff.);
- scrambling data twice (as in claim 17), -see D1 (page 22, line 25 ff.);
- data stream comprises audio visual information (as in claim 19), -see D1 (page 3, line 3 ff.);
- data stream comprises a control word (as in claim 20), see D1 (page 2, line 22 ff.);
- scrambled data stream is transmitted as part of a television broadcast (as in claim 21), see D1 (page 1);

### Inventive Step

The subject-matter of some of the dependent claims lacks inventive step as will be set out below:

Document D1 discloses (see page 22, line 19 ff.) that a double encryption may be used. It discloses that first descrambling is performed in the smartcard and the second decryption is done in the decoder. Document D1 also discusses the use of the RSA algorithm(public key- private key encryption/decryption). It is routine matter for the skilled person to replace the method of D1 by encoding the data stream in the smart-card and decoding it in the decoder by using for example the RSA algorithms. Consequently the subject-matter of claim 2 is obvious.

- first encryption key in dependence on a decoder identity (as in claim 3), -obvious to use characteristics of the host apparatus;
- encrypted communication of identity code (as in claims 4 and 5), -obvious to exchange keywords in a secure manner (see also discussion in D1, page 3, line

25 ff.);

- use of encryption keys based on random or pseudo-random numbers (as in claims 6 and 8), -common general knowledge;
- communication between decoder and security module (as in claim 7), -common general knowledge;
- encryption using keys (as in claims 9-13), -it is known to the skilled person to encode keys using e.g. a public key- private key approach;
- encryption key dependent on time and date (as in claim 16) , -obvious when confronted with the problem of limiting the decryption of data to a certain instant.

In general it is noted that the skilled person is aware (see e.g. D1) of private key- public key coding of data, multiple levels of encryption of a data stream and (partial) decoding in a smart card. The features of the claims therefore do not, even when being new over the prior art, contribute in an inventive way over the prior art. The claimed features are merely features the skilled person would apply routinely when confronted with the corresponding problem.

**VII. Certain Defects**

1. Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in document D1 are not mentioned in the description.
2. The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).
3. In order to facilitate the examination of the conformity of the amended application with the requirements of Article 34(2)(b) PCT, the applicant is requested to clearly identify the amendments carried out, no matter whether they concern amendments by addition, replacement or deletion, and to indicate the passages of the application as filed on which these amendments are based (see also Rule 66.8(a) PCT).

### VIII. Certain Observations

#### Article 6 PCT

The subject-matter of some of the claims does not fulfil the requirements of Article 6 PCT because the claims are not clear. This will be set out below:

In general it is noted that the wording of the claims is rather general and does not properly define the subject-matter to be protected. For example in claim 1 it is not clear what kind of data is transmitted and received, in particular it is not clear whether this video data, or keys for decoding encrypted data etc.. Also it is not clear what the term "portable security module" means. Many devices are portable including a vast number of devices used in signal processing. In addition the term "security" does limit the claim in any clear way since it is not clear what kind of security systems are concerned.



# PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

# PCT

To:

MATHYS & SQUIRE  
Attn. COZENS, P.  
100 Gray's Inn Road  
London WC1X 8AL  
UNITED KINGDOM

NOTIFICATION OF TRANSMITTAL OF  
THE INTERNATIONAL SEARCH REPORT  
OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing  
(day/month/year)

04/12/1998

Applicant's or agent's file reference

PDC/AB/20099

**FOR FURTHER ACTION**

See paragraphs 1 and 4 below

International application No.

PCT/IB 98/ 01610

International filing date

(day/month/year)

02/10/1998

Applicant

CANAL+ SOCIETE ANONYME et al.

1. ☒ The applicant is hereby notified that the International Search Report has been established and is transmitted herewith.

**Filing of amendments and statement under Article 19**

The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

**When?** The time limit for filing such amendments is normally 2 months from the date of transmittal of the International Search Report; however, for more details, see the notes on the accompanying sheet.

**Where?** Directly to the International Bureau of WIPO  
34, chemin des Colombettes  
1211 Geneva 20, Switzerland  
Facsimile No.: (41-22) 740.14.35

For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no International Search Report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3. ☐ With regard to the protest against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicants's request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Further action(s):** The applicant is reminded of the following:

Shortly after 18 months from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90bis.1 and 90bis.3, respectively, before the completion of the technical preparations for international publication.

Within 19 months from the priority date, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later).

Within 20 months from the priority date, the applicant must perform the prescribed acts for entry into the national phase before all designated Offices which have not been elected in the demand or in a later election within 19 months from the priority date or could not be elected because they are not bound by Chapter II.

Name and mailing address of the International Searching Authority

European Patent Office, P.B. 5818 Patentlaan 2  
NL-2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Falk Heck

## NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the PCT Applicant's Guide, a publication of WIPO.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions respectively.

### INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only.

#### What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

#### When?

Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

#### Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

#### How?

Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Administrative Instructions, Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

#### What documents must/may accompany the amendments?

##### Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

## NOTES TO FORM PCT/ISA/220 (continued)

The letter must indicate the differences between the claims as filed and the claims as amended. It must, in particular, indicate, in connection with each claim appearing in the international application (it being understood that identical indications concerning several claims may be grouped), whether

- (i) the claim is unchanged;
- (ii) the claim is cancelled;
- (iii) the claim is new;
- (iv) the claim replaces one or more claims as filed;
- (v) the claim is the result of the division of a claim as filed.

The following examples illustrate the manner in which amendments must be explained in the accompanying letter:

1. [Where originally there were 48 claims and after amendment of some claims there are 51]:  
"Claims 1 to 29, 31, 32, 34, 35, 37 to 48 replaced by amended claims bearing the same numbers; claims 30, 33 and 36 unchanged; new claims 49 to 51 added."
2. [Where originally there were 15 claims and after amendment of all claims there are 11]:  
"Claims 1 to 15 replaced by amended claims 1 to 11."
3. [Where originally there were 14 claims and the amendments consist in cancelling some claims and in adding new claims]:  
"Claims 1 to 6 and 14 unchanged; claims 7 to 13 cancelled; new claims 15, 16 and 17 added." or  
"Claims 7 to 13 cancelled; new claims 15, 16 and 17 added; all other claims unchanged."
4. [Where various kinds of amendments are made]:  
"Claims 1-10 unchanged; claims 11 to 13, 18 and 19 cancelled; claims 14, 15 and 16 replaced by amended claim 14; claim 17 subdivided into amended claims 15, 16 and 17; new claims 20 and 21 added."

### "Statement under article 19(1)" (Rule 46.4)

The amendments may be accompanied by a statement explaining the amendments and indicating any impact that such amendments might have on the description and the drawings (which cannot be amended under Article 19(1)).

The statement will be published with the international application and the amended claims.

It must be in the language in which the international application is to be published.

It must be brief, not exceeding 500 words if in English or if translated into English.

It should not be confused with and does not replace the letter indicating the differences between the claims as filed and as amended. It must be filed on a separate sheet and must be identified as such by a heading, preferably by using the words "Statement under Article 19(1)."

It may not contain any disparaging comments on the international search report or the relevance of citations contained in that report. Reference to citations, relevant to a given claim, contained in the international search report may be made only in connection with an amendment of that claim.

### Consequence if a demand for international preliminary examination has already been filed

If, at the time of filing any amendments under Article 19, a demand for international preliminary examination has already been submitted, the applicant must preferably, at the same time of filing the amendments with the International Bureau, also file a copy of such amendments with the International Preliminary Examining Authority (see Rule 62.2(a), first sentence).

### Consequence with regard to translation of the international application for entry into the national phase

The applicant's attention is drawn to the fact that, where upon entry into the national phase, a translation of the claims as amended under Article 19 may have to be furnished to the designated/elected Offices, instead of, or in addition to, the translation of the claims as filed.

For further details on the requirements of each designated/elected Office, see Volume II of the PCT Applicant's Guide.

## PATENT COOPERATION TREATY

## PCT

## INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference <b>PDC/AB/20099</b>	<b>FOR FURTHER ACTION</b> see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. <b>PCT/IB 98/ 01610</b>	International filing date (day/month/year) <b>02/10/1998</b>	(Earliest) Priority Date (day/month/year) <b>02/10/1997</b>
Applicant <b>CANAL+ SOCIETE ANONYME et al.</b>		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 2 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. ☐ Certain claims were found unsearchable (see Box I).

2. ☐ Unity of invention is lacking (see Box II).

3. ☐ The international application contains disclosure of a nucleotide and/or amino acid sequence listing and the international search was carried out on the basis of the sequence listing

☐ filed with the international application.

☐ furnished by the applicant separately from the international application.

☐ but not accompanied by a statement to the effect that it did not include matter going beyond the disclosure in the international application as filed.

☐ Transcribed by this Authority

4. With regard to the title, ☒ the text is approved as submitted by the applicant

☐ the text has been established by this Authority to read as follows:

5. With regard to the abstract,

☒ the text is approved as submitted by the applicant

☐ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this International Search Report, submit comments to this Authority.

6. The figure of the drawings to be published with the abstract is:

Figure No. 4 ☒ as suggested by the applicant.

☐ None of the figures.

☐ because the applicant failed to suggest a figure.

☐ because this figure better characterizes the invention.

## INTERNATIONAL SEARCHREPORT

International Application No

PCT/IB 98/01610

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 H04N7/16 H04N7/167

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 96 06504 A (THOMSON CONSUMER ELECTRONICS ; CHANEY JOHN WILLIAM (US)) 29 February 1996 see page 3, line 25 - page 4, line 13 see page 15, line 17 - page 17, line 6 see figures 1,4	1,2, 14-18, 20,23
A	EP 0 599 366 A (SCHLUMBERGER IND SA) 1 June 1994 see page 2, column 2, line 19 - page 3, column 3, line 19 see figure 1	1,2,20, 23



Further documents are listed in the continuation of box C.



Patent family members are listed in annex.

## \* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

23 November 1998

Date of mailing of the international search report

04/12/1998

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+31-70) 340-3016

Authorized officer

Verleye, J

## INTERNATIONAL SEARCHREPORT

Information on patent family members

International Application No

PCT/IB 98/01610

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9606504	A	29-02-1996	
		AU 3238595 A	22-03-1996
		AU 3239495 A	14-03-1996
		BR 9508621 A	30-09-1997
		BR 9508622 A	19-05-1998
		CA 2196406 A	07-03-1996
		CA 2196407 A	29-02-1996
		CN 1158202 A	27-08-1997
		CN 1158203 A	27-08-1997
		EP 0878088 A	18-11-1998
		EP 0782807 A	09-07-1997
		FI 970677 A	18-02-1997
		JP 10506507 T	23-06-1998
		JP 10505720 T	02-06-1998
		PL 318647 A	07-07-1997
		WO 9607267 A	07-03-1996
EP 0599366	A	01-06-1994	
		FR 2698510 A	27-05-1994
		AT 166761 T	15-06-1998
		DE 69318805 D	02-07-1998
		JP 6350594 A	22-12-1994
		US 5509073 A	16-04-1996

# PATENT COOPERATION TREATY

From the  
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

<b>To:</b>  COZENS, P. MATHYS & SQUIRE 100 Gray's Inn Road London WC1X 8AL GRANDE BRETAGNE	<div style="border: 2px solid black; padding: 5px; margin: 0 auto; width: 150px;"> <b>RECEIVED</b>  <b>MATHYS &amp; SQUIRE</b>    <b>04 JAN 2000</b>                  REPLY DATE 30/1/2000  <i>Report 1 PER</i>                  DIARY ENTERED             </div>	<h2 style="margin: 0;">PCT</h2>  NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT (PCT Rule 71.1)
Applicant's or agent's file reference PDC/AB/20099		Date of mailing (day/month/year) <b>30. 12. 99</b>
International application No. PCT/IB98/01610	International filing date (day/month/year) 02/10/1998	Priority date (day/month/year) 02/10/1997
Applicant CANAL+ SOCIETE ANONYME et al.		

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.
2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.
3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

#### 4. REMINDER

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/  <div style="display: flex; align-items: center;"> <div>                         European Patent Office                          D-80298 Munich                          Tel. +49 89 2399 - 0 Tx: 523656 epmu d                          Fax: +49 89 2399 - 4465                     </div> </div>	Authorized officer  Stannartz, B  Tel. +49 89 2399-8242
--	---





# PATENT COOPERATION TREATY

## PCT

### INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference <b>PDC/AB/20099</b>	<b>FOR FURTHER ACTION</b> See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. <b>PCT/IB98/01610</b>	International filing date (day/month/year) <b>02/10/1998</b>	Priority date (day/month/year) <b>02/10/1997</b>
International Patent Classification (IPC) or national classification and IPC <b>H04N7/16</b>		
Applicant <b>CANAL+ SOCIETE ANONYME et al.</b>		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.



2. This REPORT consists of a total of 9 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand  <b>16/04/1999</b>	Date of completion of this report  <b>30. 12. 99</b>
Name and mailing address of the international preliminary examining authority:   <b>European Patent Office</b> <b>D-80298 Munich</b> <b>Tel. +49 89 2399 - 0 Tx: 523656 epmu d</b> <b>Fax: +49 89 2399 - 4465</b>	Authorized officer  <b>Schoeyer, M</b>  <b>Telephone No. +49 89 2399 2136</b> 



# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/IB98/01610

## I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

### Description, pages:

1-19 as originally filed

### Claims, No.:

1-23 as originally filed

### Drawings, sheets:

1/5-5/5 as originally filed

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

## III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non-obvious), or to be industrially applicable have not been examined in respect of:

- ☐ the entire international application.
- ☒ claims Nos. 22,23.

because:

# INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/IB98/01610

☐ the said international application, or the said claims Nos. relate to the following subject matter which does not require an international preliminary examination (*specify*):

☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. are so unclear that no meaningful opinion could be formed (*specify*):

**see separate sheet**

☐ the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed.

☐ no international search report has been established for the said claims Nos. .

## V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

### 1. Statement

Novelty (N)	Yes:	Claims 2-13,16,18
	No:	Claims 1, 14,15,17,19,20,21
Inventive step (IS)	Yes:	Claims
	No:	Claims 2-13,16,18
Industrial applicability (IA)	Yes:	Claims 1-21
	No:	Claims

### 2. Citations and explanations

**see separate sheet**

## VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

**see separate sheet**

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT**

International application No. PCT/IB98/01610

---

**VIII. Certain observations on the international application**

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

**see separate sheet**

**III. Non Establishment of Opinion**

The subject-matter of claims 22 and 23 is not defined in a proper way. None of the features of these claims actually define any subject-matter.

In the case of claim 22 it has not been claimed in what way the decoder and portable security module are adapted, while in claim 23 reference is made to application as a whole without defining any subject-matter to be protected.

**V. Statement under Article 35(2) PCT**

Reference is made to the following documents:

D1: WO 96 06504 A (THOMSON CONSUMER ELECTRONICS ;CHANEY JOHN WILLIAM (US)) 29 February 1996;

**Article 33(2) PCT**

As far as the subject-matter of the claims can be understood (see under VIII), independent claim 1 does not fulfil the requirements of Article 33(2) PCT because the subject-matter of independent claim 1 is not novel.

Document D1 (see abstract) is concerned with a method of transmission and reception of a scrambled data streams and discloses:

- transmission of the scrambled data stream to a decoder and passing it on to and descrambling by a portable security module inserted in the decoder;
- passing of data stream from the security module to the decoder in an encrypted for, to be decrypted and subsequently used by the decoder.

Since these are the features of claim 1, the subject-matter of claim 1 lacks novelty.

Dependent claims:

The subject-matter of some of the dependent claims also lacks novelty as will be set out below:

Claim 14:

Document D1 discloses (see page 22), that the signal is encrypted with a key at transmission and decrypted in the receiver with the equivalent decryption key;

- encryption based on variable known to both the transmitter and the decoder (as in claim 15), -see D1 (page 2, line 22 ff.);
- scrambling data twice (as in claim 17), -see D1 (page 22, line 25 ff.);
- data stream comprises audio visual information (as in claim 19), -see D1 (page 3, line 3 ff.);
- data stream comprises a control word (as in claim 20), see D1 (page 2, line 22 ff.);
- scrambled data stream is transmitted as part of a television broadcast (as in claim 21), see D1 (page 1);

### **Inventive Step**

The subject-matter of some of the dependent claims lacks inventive step as will be set out below:

Document D1 discloses (see page 22, line 19 ff.) that a double encryption may be used. It discloses that first descrambling is performed in the smartcard and the second decryption is done in the decoder. Document D1 also discusses the use of the RSA algorithm(public key- private key encryption/decryption). It is routine matter for the skilled person to replace the method of D1 by encoding the data stream in the smart-card and decoding it in the decoder by using for example the RSA algorithms. Consequently the subject-matter of claim 2 is obvious.

- first encryption key in dependence on a decoder identity (as in claim 3), -obvious to use characteristics of the host apparatus;
- encrypted communication of identity code (as in claims 4 and 5), -obvious to exchange keywords in a secure manner (see also discussion in D1, page 3, line

**INTERNATIONAL PRELIMINARY  
EXAMINATION REPORT - SEPARATE SHEET**

---

International application No. PCT/IB98/01610

25 ff.);

- use of encryption keys based on random or pseudo-random numbers (as in claims 6 and 8), -common general knowledge;
- communication between decoder and security module (as in claim 7), -common general knowledge;
- encryption using keys (as in claims 9-13), -it is known to the skilled person to encode keys using e.g. a public key- private key approach;
- encryption key dependent on time and date (as in claim 16) , -obvious when confronted with the problem of limiting the decryption of data to a certain instant.

In general it is noted that the skilled person is aware (see e.g. D1) of private key- public key coding of data, multiple levels of encryption of a data stream and (partial) decoding in a smart card. The features of the claims therefore do not, even when being new over the prior art, contribute in an inventive way over the prior art. The claimed features are merely features the skilled person would apply routinely when confronted with the corresponding problem.

**VII. Certain Defects**

1. Contrary to the requirements of Rule 5.1(a)(ii) PCT, the relevant background art disclosed in document D1 are not mentioned in the description.
2. The features of the claims are not provided with reference signs placed in parentheses (Rule 6.2(b) PCT).
3. In order to facilitate the examination of the conformity of the amended application with the requirements of Article 34(2)(b) PCT, the applicant is requested to clearly identify the amendments carried out, no matter whether they concern amendments by addition, replacement or deletion, and to indicate the passages of the application as filed on which these amendments are based (see also Rule 66.8(a) PCT).

### **VIII. Certain Observations**

#### Article 6 PCT

The subject-matter of some of the claims does not fulfil the requirements of Article 6 PCT because the claims are not clear. This will be set out below:

In general it is noted that the wording of the claims is rather general and does not properly define the subject-matter to be protected. For example in claim 1 it is not clear what kind of data is transmitted and received, in particular it is not clear whether this video data, or keys for decoding encrypted data etc.. Also it is not clear what the term "portable security module" means. Many devices are portable including a vast number of devices used in signal processing. In addition the term "security" does limit the claim in any clear way since it is not clear what kind of security systems are concerned.





20099

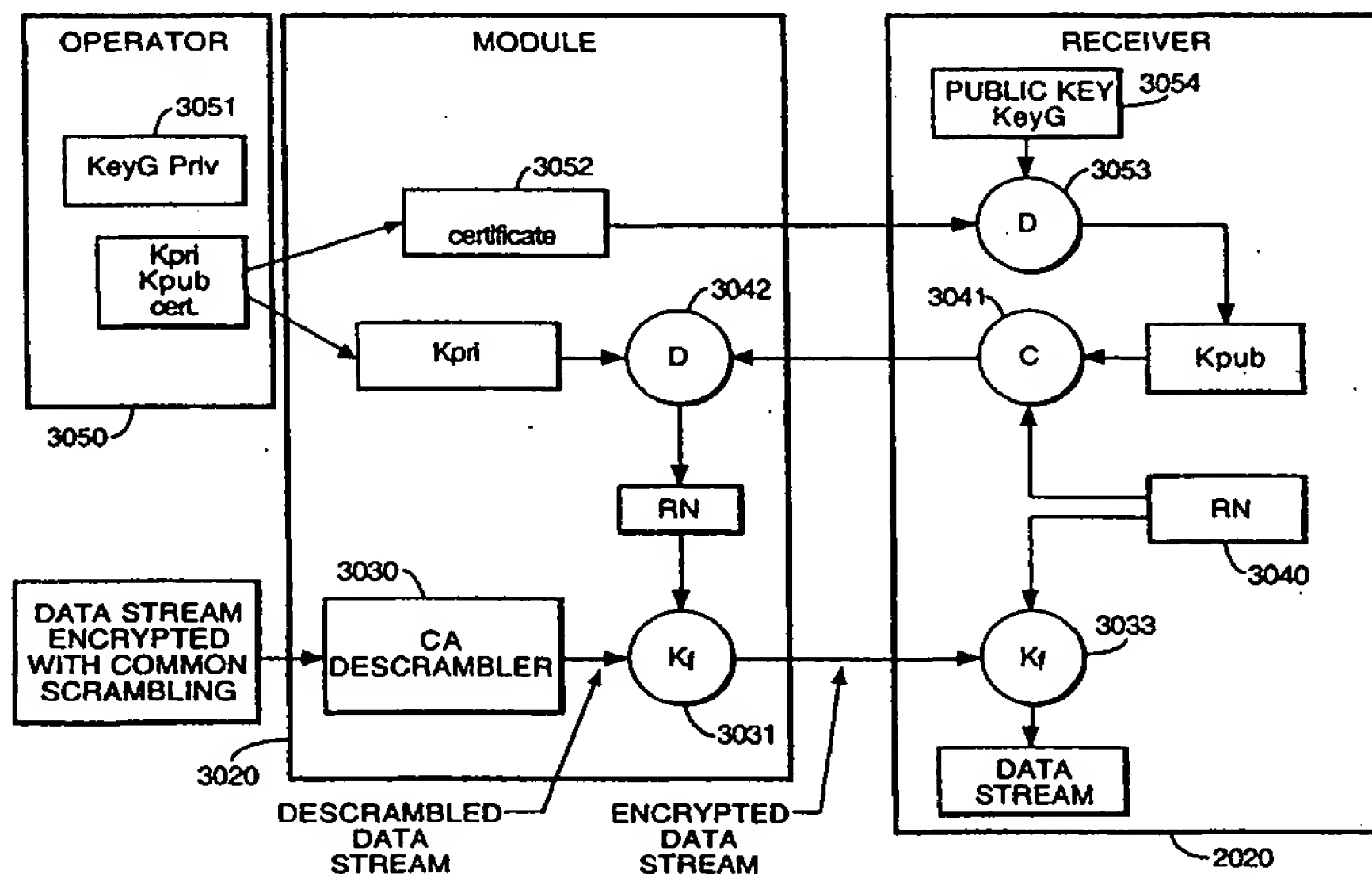
## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification <sup>6</sup> : <b>H04N 7/16, 7/167</b>		<b>A1</b>	(11) International Publication Number: <b>WO 99/18729</b>
			(43) International Publication Date: 15 April 1999 (15.04.99)
(21) International Application Number: PCT/IB98/01610		(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).	
(22) International Filing Date: 2 October 1998 (02.10.98)			
(30) Priority Data:			
97402322.8	2 October 1997 (02.10.97)	EP	
98401388.8	9 June 1998 (09.06.98)	EP	
98401389.6	9 June 1998 (09.06.98)	EP	
(71) Applicant (for all designated States except US): CANAL+ SOCIETE ANONYME [FR/FR]; 85/89, quai André-Citroen, F-75711 Paris Cedex 15 (FR).			
(72) Inventors; and			
(75) Inventors/Applicants (for US only): MAILLARD, Michel [FR/FR]; 42, avenue du Maréchal-Leclerc, F-28130 Maintenon (FR). BENARDEAU, Christian [FR/FR]; 13, allée des Puisatiers, F-77600 Bussy-Saint-Georges (FR). DAUVOIS, Jean-Luc [FR/FR]; 19, rue Eugène-Manuel, F-75116 Paris (FR).			
(74) Agents: COZENS, Paul, Dennis et al.; Mathys & Squire, 100 Grays Inn Road, London WC1X 8AL (GB).			

Published

With international search report.

(54) Title: METHOD AND APPARATUS FOR ENCRYPTED DATA STREAM TRANSMISSION



## (57) Abstract

A method of transmission and reception of scrambled data in which the scrambled data is transmitted to a decoder (2020), the scrambled data being passed to and descrambled by a security module or smart card (3020) inserted in the decoder (2020) and characterised in that the scrambled data stream is passed from the smart card (3020) back to the decoder (3020) in an encrypted form. The encryption of the data stream may be carried out on the card (3020) or as a secondary encryption step at transmission. The data stream may correspond directly to audiovisual data descrambled in the security module or to a stream of control word data subsequently used by the decoder to descramble a transmission.